PATENT COOPERATION TREATY

PCT

REC'D 11 APR 2006

WIPO   PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P14068/MA	FOR FURTHER ACTION		See Form PCT/IPEA/416
International application No. PCT/EP2005/050547	International filing date *(day/month/year)* 08.02.2005		Priority date *(day/month/year)* 11.02.2004

International Patent Classification (IPC) or national classification and IPC

INV. H04L29/06

Applicant

SONY ERICSSON MOBILE COMMUNICATIONS AB et al.

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

3. This report is also accompanied by ANNEXES, comprising:

   a. ☒ *sent to the applicant and to the International Bureau)* a total of 1-5 sheets, as follows:

   ☒ sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).

   ☐ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.

   b. ☐ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or tables related thereto, in celectronic form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).

4. This report contains indications relating to the following items:

   ☒ Box No. I   Basis of the report

   ☐ Box No. II   Priority

   ☐ Box No. III   Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

   ☐ Box No. IV   Lack of unity of invention

   ☒ Box No. V   Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

   ☐ Box No. VI   Certain documents cited

   ☐ Box No. VII   Certain defects in the international application

   ☐ Box No. VIII   Certain observations on the international application

Date of submission of the demand 09.12.2005	Date of completion of this report 11.04.2006

Name and mailing address of the international preliminary examining authority:
    European Patent Office - P.B. 5818 Patentlaan 2
    NL-2280 HV Rijswijk - Pays Bas
    Tel. +31 70 340 - 2040 Tx: 31 651 epo nl
    Fax: +31 70 340 - 3016
	Authorized officer
	
	Veen, G
	
	Telephone No. +31 70 340-3811

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

Box No. I   Basis of the report

1. With regard to the **language**, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

   ☐   This report is based on translations from the original language into the following language , which is the language of a translation furnished for the purposes of:

   ☐   international search (under Rules 12.3 and 23.1(b))
   ☐   publication of the international application (under Rule 12.4)
   ☐   international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the **elements*** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

   Description, Pages

   1-11   as originally filed

   Claims, Numbers

   1-34   filed with telefax on 09.12.2005

   Drawings, Sheets

   1/5-5/5   as originally filed

   ☐   a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing

3. ☐   The amendments have resulted in the cancellation of:
   ☐   the description, pages
   ☐   the claims, Nos.
   ☐   the drawings, sheets/figs
   ☐   the sequence listing *(specify)*:
   ☐   any table(s) related to sequence listing *(specify)*:

4. ☐   This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).
   ☐   the description, pages
   ☐   the claims, Nos.
   ☐   the drawings, sheets/figs
   ☐   the sequence listing *(specify)*:
   ☐   any table(s) related to sequence listing *(specify)*:

   *   If item 4 applies, some or all of these sheets may be marked "superseded."

Box No. V   Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-34
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-34
Industrial applicability (IA)	Yes:	Claims	1-34
	No:	Claims	

2. Citations and explanations (Rule 70.7):

   see separate sheet

Re Item V
Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Reference is made to the following documents:

D1: EP-A-1 361 527 (SONY ERICSSON MOBILE COMM AB) 12 November 2003 (2003-11-12)

D2: EP-A-1 262 859 (CANON KK) 4 December 2002 (2002-12-04)

D3: EP-A-1 004 992 (VISA INT SERVICE ASS) 31 May 2000 (2000-05-31)

D4: WO 02/067173 A (CHAN KIM HING ; GU GUOLIANG (SG); SPRINT INNOVATIONS PTE LTD I (SG)) 29 August 2002 (2002-08-29)

1   The present application does not meet the requirements of Article 33(1) PCT, because the subject-matter of independent claims 1 and 18 does not involve an inventive step in the sense of Article 33(3) EPC.

1.1   Using the words of independent claim 1 of the present application and taking references from D1, D1 discloses:

"A method of providing a dynamic security management in an apparatus comprising: a platform for running an application (colum 2 lines 37-39); a security manager (c3l20-22) for handling access of the application to functions existing in the apparatus (c2l51-53); an application interface between the platform and the application (c2l53-54); a set of access permissions (c3l22) stored in the apparatus (c3l23) and used by the security manager for controlling access of the application to functions through the application interface (§21), **characterised** by the steps of:
downloading into the apparatus an object containing access permissions applicable to at least one function (c2l50-51; c3l57-c4l2), said object comprising new routines and/or new functions (c2l39-40);
verifying the object (c2l48-49);
installing the access permissions together with the existing permissions (c3l25-28; c3lc57-c4l2); ~~said object enhancing the application interface with said new routines and/or new functions~~"

Claim 1 thus differs from D1 in that the downloaded object enhances the application interface with said new routines and functions.

Ignoring the fact that this feature, more specifically the expression "enhancing the application interface", is not clear, D1 does not imply any restrictions on the kind of functions or applications which are downloaded. Therefore, this feature cannot be considered so as to render the present application inventive (Art. 33(3) PCT).

2   The same reasoning applies, mutatis mutandis, to the subject-matter of corresponding independent claims 14, 17 and 30, respectively, which are therefore also not inventive.

3   Dependent claims 2-13, 15, 16, 18-29 and 31-34 do not contain any features which, in combination with the features of the respective claims to which they refer, meet the requirements of the PCT in respect of novelty and inventive step, see D1-D4.

12

CLAIMS

1. A method of providing a dynamic security management in an apparatus (1) comprising: a platform for running an application (2); a security manager (7) for handling access of the application (2) to functions (3) existing in the apparatus; an application interface (11A) between the platform and the application (2); a set of access permissions stored in the apparatus and used by the security manager (7) for controlling access of the application (2) to functions (3) through the application interface (11A), **characterised** by the steps of:
    downloading into the apparatus (1) an object containing access permissions applicable to at least one function (3) said object comprising new routines and/or new functions;
    verifying the object;
    installing the access permissions together with the existing permissions;
    said object enhancing the application interface (11A) with said new routines and/or new functions.

2. A method according to claim 1, **characterised** in that the object is verified by checking a certificate chain of the object.

3. A method according to claim 1 or 2, **characterised** in that it is verified that a policy (8) of the function allows updates.

4. A method according to any one of the previous claims, **characterised** by downloading a further object containing a library (12), or the downloaded object further containing a library (12), said library (12) comprising new routines and/or new functions to be called by an application or library stored in the apparatus; and installing the library (12) to enable access of functions (3) through the application interface (11A).

5. A method according to claim 4, **characterised** in that the new routines and/or new functions can access existing functions through a library (12).

6. A method according to claim 5, **characterised** in that the security manger (7), when accessing functions, recursively checks the permissions of the application interfaces (11A, 11B) and libraries (12) in a linked chain related to the called functions (3).

7. A method according to any one of the previous claims, **characterised** by

13

downloading a further object containing an application (2), or the downloaded object further containing an application (2), said application (2) containing at least one new function; and installing the new function so that the new function can access existing functions through the application interface (11A).

5

8. A method according to claim 7, **characterised** in that the new functions can access existing functions through a library (12).

9. A method according to any one of the previous claims, **characterised** in that the access permissions are contained in a policy file.

10

10. A method according to claim 9, **characterised** in that the policy file has a structure linking access levels of existing functions with a domain associated with the downloaded object.

15

11. A method according to claim 9 or 10, **characterised** in that the policy file has a structure linking access levels of existing functions with information contained in a certificate chain.

20 12. A method according to claim 11, **characterised** in that the information includes signature of the end entity certificate, signature of an intermediate certificate, or specific level information (level OID).

13. A method according to claim 10 or 11, **characterised** in that the policy file has a structure including logical expressions.

25

14. A method of providing a dynamic security management in an apparatus (1) comprising: a platform for running an application (2); a security manager (7) for handling access of the application (2) to functions (3) existing in the apparatus; an application interface (11A) between the platform and the application (2); a set of access permissions stored in the apparatus and used by the security manager (7) for controlling access of the application (2) to functions (3) through the application interface (11A), **characterised** by the steps of:

30

storing the access permissions in a security policy (8);
providing the security policy (8) with a hierarchical structure, wherein the security policy (8) has a structure linking access levels of existing functions with a domain associated with the downloaded object, the domain defining the basic access level which may be combined with other information.

35

14

15. A method according to claim 14, **characterised** in that the security policy (8) has a structure linking access levels of existing functions with information contained in a certificate chain.

5

16. A method according to claim 15, **characterised** in that the information includes signature of the end entity certificate, signature of an intermediate certificate, or specific level information (level OID).

10 17. An apparatus (1) with dynamic security management comprising: a platform for running an application (2); a security manager (7) for handling access of the application (2) to functions (3) existing in the apparatus (1); an application interface (11A) between the platform and the application (2); a set of access permissions stored in the apparatus and used by the security manager (7) for

15 controlling access of the application (2) to functions (3) through the application interface (11A), **characterised** in that:
the apparatus (1) is arranged to download an object containing access permissions applicable to at least one function (3), said object comprising new routines and/or new functions;

20 to verify the object; and
to install the access permissions together with the existing permissions;
said object enhancing the application interface (11A) with said new routines and/or new functions.

25 18. An apparatus according to claim 17, **characterised** in that the security manager (7) is adapted to verify the object by checking a certificate chain of the object.

19. An apparatus according to claim 17 or 18, **characterised** in that the security

30 manager (7) is adapted to verify that a policy of the function allows updates.

20. An apparatus according to any one of claims 17 to 19, **characterised** in that the apparatus is arranged to download a further object containing a library (12), or the downloaded object further containing a library (12), said library

35 (12) comprising new routines and/or new functions to be called by an application (2) or library (12) stored in the apparatus; and to install the library (12) to enable access of functions through the application interface (11A).

21. An apparatus according to claim 20, **characterised** in that the new routines

15

and/or new functions can access existing functions through a library (12).

22. An apparatus according to claim 21, **characterised** in that the security manger (7), when accessing functions, is adapted to recursively check the permissions of the application interfaces (11A, 11B) and libraries (12) in a linked chain related to the called functions

23. An apparatus according to any one claims 17 to 22, **characterised** in that the apparatus is arranged to download a further object containing an application (2), or the downloaded object further containing an application (2), said application (2) containing at least one new function; and to install the new function so that the new function can access existing functions through the application interface (11A).

24. An apparatus according to claim 23, **characterised** in that the new functions can access existing functions through a library (12).

25. An apparatus according to any one of claims 17 to 24, **characterised** in that the access permissions are contained in a policy file.

26. An apparatus according to claim 25, **characterised** in that the policy file has a structure linking access levels of existing functions with a domain associated with the downloaded object.

27. An apparatus according to claim 25 or 26, **characterised** in that the policy file has a structure linking access levels of existing functions with information contained in a certificate chain.

28. An apparatus according to claim 27, **characterised** in that the information includes signature of the end entity certificate, signature of an intermediate certificate, or specific level information (level OID).

29. An apparatus according to claim 27 or 28, **characterised** in that the policy file has a structure including logical expressions.

30. An apparatus (1) with dynamic security management comprising: a platform for running an application (2); a security manager (7) for handling access of the application (2) to functions (3) existing in the apparatus; an application interface (11A) between the platform and the application (2); a set of access

16

permissions stored in the apparatus and used by the security manager (7) for controlling access of the application (2) to functions (3) through the application interface (11A), **characterised** in that the apparatus is arranged to: store the access permissions in a security policy (8);

5   provide the security policy (8) with a hierarchical structure.

31.   An apparatus according to claim 30, **characterised** in that the security policy (8) has a structure linking access levels of existing functions with a domain associated with the downloaded object.

10

32.   An apparatus according to claim 31, **characterised** in that the security policy (8) has a structure linking access levels of existing functions with information contained in a certificate chain.

15   33.   An apparatus according to claim 32, **characterised** in that the information includes signature of the end entity certificate, signature of an intermediate certificate, or specific level information (level OID).

34.   An apparatus according to any one of claims 17 to 33, **characterised** in that
20   the apparatus (1) is a portable telephone, a pager, a communicator, a smart phone, or an electronic organiser.